



Security Incident
Guidelines for Offshore
Installations Managers
(OIMs)

Guidelines

Acknowledgments

While every effort has been made to ensure the accuracy of the information contained in this publication, neither Oil & Gas UK, nor any of its members will assume liability for any use made of this publication or the model agreement to which it relates.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without prior written permission of the publishers.

Crown copyright material is reproduced with the permission of the Controller of Her Majesty's Stationery Office.

Copyright © 2020 The UK Oil and Gas Industry Association Limited trading as Oil & Gas UK

ISBN: 978-1-913078-27-0

PUBLISHED BY OIL & GAS UK

London Office:

6th Floor East, Portland House, Bressenden Place, London, SW1E 5BH
Tel: 020 7802 2400 Fax: 020 7802 2401

Aberdeen Office:

Exchange 2, 3rd Floor, 62 Market Street, Aberdeen, AB11 5PJ
Tel: 01224 577250 Fax: 01224 577251

info@oilandgasuk.co.uk

www.oilandgasuk.co.uk

Security Incident Guidelines for Offshore Installations Managers (OIMs)

February 2020

Contents

1	Outline	5
1.1	Introduction	5
1.2	Primary Parties in an Offshore Security Incident	6
1.2.1	OIMS	6
1.2.2	Onshore Team	6
1.2.3	Police (or other relevant authority)	6
2	Responsibility of the OIM	7
2.1	Initial Incident Responsibilities	7
3	Powers of Restraint	9
3.1	Offshore Installation and Pipeline Works (Management and Administrations) Regulations 1995, Regulation 7	9
3.2	Merchant Shipping Act 1995, Section 105	9
3.3	The Ship and Port Facility (Security) Regulations 2004	9
4	Further Actions that may be Undertaken	10
4.1	Witnesses	10
4.2	Suspects	10
4.3	Seizure	11
4.4	Photography	11
5	Further Information	12
5.1	Major Incident Box Content	12
5.2	Specimen Incident Log	12
5.3	Evidence Definitions	13
6	Procedure for OIMs in the event of a crime or security incident	15
7	Cyber Security	17
8	Firearms Guidance	19
9	Appendix	22
	Appendices	23
A	Bomb Threat Procedures	23
B	Suspect Package / Item	26
C	Drugs / Contraband Find	28

D	Hostage Situation	29
E	Sabotage / Criminal Damage	30
F	Assault	31
G	Illegal Occupation	32
H	Sudden Death	35
I	Armed Assailant Action	38

1 Outline

1.1 Introduction

Offshore Installation Managers (OIMs) have primary responsibility for the safety of their installation and the Personnel On Board (POB). As such, it is important to ensure that procedures are in place and OIMs are trained, to provide the initial management of any security incident. These guidelines aim to provide assistance to operators and a practical reference to their OIMs or their deputies in the event of, an alleged, violent crime¹ or security-related incident occurring offshore. It is intended that these guidelines are consistent with the requirements of the Police should they be unable to attend the scene or there is a significant delay in their presence. It should be noted, however, that these guidelines are not prescriptive and do not provide for every situation.

When Health & Safety Executive (HSE) is involved in investigating any work-related death, inspectors will work closely with other Regulators and the Police. To help to do this protocols and liaison arrangements between the various organisations are recorded in Work-Related Deaths Protocols (WRDP). These protocols can be found on the HSE website:

<http://www.hse.gov.uk/enforce/wrdp/index.htm>

These guidelines are divided into two parts: firstly, the body of the guidelines provides operators with information on areas that they may wish to consider in developing their own procedures; and secondly, the appendices provide template procedures that operators may wish to adopt or use as a base for their own procedure. Further, it is acknowledged that some operators will already have fit-for-purpose internal procedures to identify the circumstances which will trigger an internal investigation, the purpose of an investigation, how it should be conducted and by whom. These guidelines are not intended to supersede or replace a company's own policies and procedures.

Fundamental to these guidelines is the premise that the OIM should make contact with their onshore team, who will be responsible for contacting and liaising with the Police. The OIM should be aware that the Police may request a copy of the operator's internal investigation report, on a voluntary basis or may take possession of a copy on production of an appropriate search warrant, as part of their investigation. The extent of any voluntary co-operation between an operator and the Police is matter for each individual operator and may be affected by matters such as legal privilege.

¹ Note that the reference to "violent crime" means that these Guidelines do not cover offences arising from health and safety work related injuries. It is noted that, on occasions, it may be difficult to determine whether an incident is a health and safety work related incident. In such circumstances then the scene should be contained and preserved. Further guidance should be sought from the onshore team.

1.2 Primary Parties in an Offshore Security Incident

1.2.1 OIMS

The OIM is in overall charge of an installation and in the event of a security incident offshore, the OIM's primary responsibility is to secure the safety of the installation and the personnel on board. The OIM should contact his onshore team at the earliest opportunity and await instruction from them; however the OIM by nature of his unique position has a key role in the co-ordination and management of any incident.

1.2.2 Onshore Team

The onshore team should at the earliest opportunity, and as a matter of priority, establish liaison with the Police. The onshore team should act as a conduit between the Police and the OIM to ensure that the OIM receives all necessary and relevant information and direction to provide the best incident management until the Police arrive. Where the Police decide not to attend the scene, this should be communicated to the OIM.

1.2.3 Police (or other relevant authority)

The Police will take primacy for all criminal matters and other investigations involving death or serious injury; this may involve a joint investigation with the HSE where the incident is "work related". The Police should establish communication with the relevant onshore personnel as quickly as possible to ensure that accurate and succinct directions can be communicated to the OIM, including information on whether or not the Police will attend offshore. When the Police attend offshore they will liaise with the OIM, recognising that the OIM is in charge of the installation and responsible for overall safety, to ensure that any investigation is undertaken in the safest manner possible.

2 Responsibility of the OIM

The severity of the incident will determine the nature of the initial response and its subsequent management. It is important that the OIM endeavours to act objectively and fairly from the outset.

It is accepted that the OIM is not an expert in the management of criminal incidents. The management and examination of scene should be left to the professional experts and the OIM should follow the instructions from his onshore team (who will be liaising with the Police). Such instructions should take the form below.

Where the Police attend offshore then the OIM will remain in charge of the installation but will be advised by the Police on their requirements. The OIM should aim to provide assistance as necessary but may wish to consult with his/her onshore team.

2.1 Initial Incident Responsibilities

Secure the safety of the installation and POB – this is the primary responsibility of the OIM. Wherever possible, all personnel should be removed from the scene. Details on powers of restraint can be found below;

Contain and preserve the scene – the scene should be protected from unauthorised entry and the elements. In order to do this, the OIM should consider the following:

- i. **Preserve** – If the scene is, or is at risk of being, exposed to the elements then a structure covering as large an area as possible should be erected taking into account the safe running of the installation. The saving of life is paramount to other considerations. Where a life is capable of being saved then this should be the primary consideration. It maybe that a course of action must be taken that may disturb the scene and, as such, the OIM must be aware that any interference with the scene may also alter the significance to be attached to other evidential items located there. If any such action is taken then it is imperative that the actions and the reason for such actions, are recorded in the incident log book. If the matter is not time critical then the onshore team should be consulted;
- ii. **Isolate** - The area should be isolated provided this can be done without compromising the crew's safety and it is not critical to the ongoing operations of the installation. It should be protected from unauthorised entry using available staff resources. Barriers should be secured notes made on what was found at the scene and actions taken until the arrival of the Police;
- iii. **Secure** - Ensure the area is secure; for example, using available staff to maintain a watch on areas where others could enter the scene. Where the scene is of a distressing nature, all efforts should be made to prevent crew members viewing the scene; and
- iv. **Evidence** - Treat any incident scene with the utmost importance and keep an incident log book. This will allow the OIM to detail their courses of action and the reasons why. On arrival, the Police will conduct a detailed examination of the crime scene and it is therefore essential that the above points are observed; and

- v. **People** – Take note of who was at the scene upon discovery of the scene and who has been involved in containing and preserving the scene.

Once these initial responsibilities have been undertaken, the OIM should await further instruction from the onshore team or until the arrival of the Police. The template procedures annexed to these guidelines outlines further information on actions that could be taken by the OIM; however the OIM should only take further action if the Police and onshore team think it prudent to do so.

3 Powers of Restraint

3.1 Offshore Installation and Pipeline Works (Management and Administrations) Regulations 1995, Regulation 7

If an installation manager has reasonable cause to believe that it is necessary or expedient to do so for the purposes of securing safety of the offshore installation or the safety or health of persons on or near it, he may take such measures against a person on the installation, including:

- restraint of this person; and
- putting him ashore in the United Kingdom as soon as practicable thereafter, as are reasonable.

If it appears likely that a person will not be put ashore within twenty-four hours of being put under restraint, the installation manager shall forthwith give notice to the duty holder of this being kept under restraint and of the reason for it.

3.2 Merchant Shipping Act 1995, Section 105

The master of any United Kingdom ship [this includes mobile drilling units (MODUs), drill ships, flotels and Floating Production Storage Offloading (FPSOs)] may cause any person on board the ship to be put under restraint if and for so long as it appears to him necessary or expedient in the interest of safety or for the preservation of good order or discipline on board the ship.

3.3 The Ship and Port Facility (Security) Regulations 2004

With regards to restricted areas on a mobile installation or support ship, there are relevant powers within:-The Ship and Port Facility (Security) Regulations 2004:

Part 4 refers to “Unauthorised presence in a restricted area of a ship” and Regulation 10 (4) states: “A constable, or the master, or the ship security officer, or a person acting on behalf of the master or the ship security officer, may use such force as is reasonable in the circumstances to remove from a restricted area a person remaining in it in contravention of paragraph (1) (b).”

For all of the above powers it is vital that the OIM keeps an incident log book so that it can be referred to if they are subsequently required to justify any particular course of action. Should the OIM decide to use these powers of restraint, the following should be considered by the OIM:

- Have all other options been exhausted (e.g. communication skills, verbal commands)?
- Only the minimum amount of force required should be used. It is vitally important to ensure also that those assisting the OIM are fully aware of this and do not, under any circumstances, exceed the minimum force required. Anyone exceeding their powers may face criminal allegations.
- Precise details of the incident must be logged, in the incident log book, including the conduct of the aggressor, the methods used to try to defuse the situation, the method of restraint used, those involved in assisting the OIM, and the outcome.

4 Further Actions that may be Undertaken

Upon the direction of the onshore team, the OIM may be requested to undertake further actions. This will be dependent upon the levels of co-operation agreed between the operator and the Police, and also whether or not the Police intend to visit the installation:

4.1 Witnesses

OIMS may be asked to:

- **Identify** – try and make a list of personnel who may have witnessed the incident, either directly or indirectly. It should be noted, however, that the identification of all relevant witnesses in a Police investigation is the responsibility of the Police. Please note that any list would be compiled for the primary purpose of supporting the operator’s internal investigation. However, the Police may request it be handed over to them on a voluntary basis or they may take possession of it on production of an appropriate search warrant.
- **Isolate** - It is good practice to suggest to potential witnesses that they do not discuss what they witnessed, as any discussion amongst them could result in statements which include speculation and a mixture of what the witness actually saw and what others saw. The OIM may consider suggesting to potential witnesses that they may wish to write down their version of events while it remains fresh in their minds, although he cannot insist on such action. Please note this record of events will belong to the individual concerned and will be for their reference going forward. If the operator wishes to keep copies of these records then this should be made clear to the individuals concerned prior to the record being made. In addition, the Police may request such records be handed over to them on a voluntary basis or they may take possession of it on production of an appropriate search warrant.
- **Interview** – The Police are responsible for interviewing witnesses as part of a Police investigation. Company interviews may be carried out, at the request of the onshore team, to establish the facts or whether the incident is serious enough to request the Police to attend offshore. These will, however, be the property of the operator. No action should be taken without instruction from the onshore team and any company interview should be conducted in the presence of another person not involved in the incident.

4.2 Suspects

Suspects are innocent until their guilt is proven. When the Police are to attend the operator’s installation, the OIM should liaise with the onshore team. The Police have the responsibility of identifying and interviewing suspects as part of a Police investigation.

Without prejudice to the powers of restraint described in Section 3 above, where the OIM believes there to be an obvious suspect, it may be prudent to ask that person to agree to remain separate from the rest of the workforce and agree to be accompanied by at least two people. This is to help ensure that evidence is not tampered with or destroyed (e.g. disposal of a weapon in the case of an assault or stabbing) whilst ensuring the safety of those accompanying the suspect.

4.3 Seizure

Police have power at Common Law to seize evidence without warrant. An OIM may, in order to protect the safety of the installation and its POB, take items such as weapons and retain them safely until they are taken by the Police. No other items should be taken without the prior consultation of the onshore team.

4.4 Photography

Photography should be left to the Police when they arrive at the installation. In the event the Police decided that they will not attend the installation then, as part of the internal investigation, the OIM may be requested to photograph the scene. Advice should be sought from the onshore team as to the appropriate procedures to be undertaken; however the general principle in photographing any scene is that care should be taken to avoid any disruption or contamination of the scene.

If the photographs are taken by the OIM then they will be owned by the operator. The Police may request such records be handed over to them on a voluntary basis or they may take possession of them through production of an appropriate search warrant.

5 Further Information

5.1 Major Incident Box Content

Every installation should have a Major Incident Box, which should be regularly maintained and kept in a readily accessible location. The following items should be included (as a minimum) in each box:

- Incident log books
- Quantity of pens (including marker pens)
- Clip boards
- Labels/tags
- Rolls of incident cordon tape
- Surgical gloves (disposable)
- Large pair of scissors
- Large brown paper sacks
- Plastic bags with seals for storage of drugs
- White paper suits for entry to scene and for suspect if clothes are to be seized
- Cardboard boxes (various sizes) for storage of evidential items such as weapons
- Plastic cover shoes
- Digital camera
- Torches
- Digital tape recorder
- Tent/cover sheet for protection from weather

5.2 Specimen Incident Log

An incident log should be maintained for all incidents. This provides the ability to produce accurate and contemporaneous records of an incident as evidence in the event of a post incident investigation. A specific incident log book should be kept and should be separate from the platform log. Example specimen log can be found below:

SPECIMEN LOG

INCIDENT LOG.....

TIME COMMENCED.....

LOG KEPT BY.....

Serial Number	Date / Time	Occurrence/Decision	Reference to other entries	Actions
1	05/ 0010	Informed of body in canteen by Ron Smith.		
2	0011	Asked medic to go to area outside canteen and to meet me there.		
3	0014	Medic John Roberts informs me that he believes the male person is dead and it is the body of Joseph Wall (yet to be confirmed). Body has what appears to be a stab wound to the chest and a knife is lying nearby.		
4	0018	Contacted onshore team.		
5	0020	Photograph of body taken following advice from onshore team.		
6	0021	Canteen and area cordoned off with tape and Paul Williams posted to keep people out of the canteen area.		
7	0030	Detective Chief Inspector Jones contacted/gave following adviceetc.	See 4 above	

5.3 Evidence Definitions

The laws relating to evidence are complex and it is the responsibility of the Police to ensure that correct procedures are followed. Nevertheless, there may be occasions when the Police do not attend offshore and ensuring a chain of actions/ownership is important.

If the Police are to attend offshore, unnecessary handling of evidence should be avoided and, where practicable, items should be left where they are until arrival of the Police. The correct labelling and packaging of evidence as part of a Police investigation is the responsibility of the Police.

If following discussions with the Police the OIM is requested to collect the evidence the Police may assist by giving instructions on what notes and actions should be taken. These instructions will include noting where the exhibit was found, by whom, who packaged it and the details of the person completing the label. Details of where it was stored after seizure should be recorded in the incident log book.

6 Procedure for OIMs in the event of a crime or security incident

This procedure aims to provide OIMs with information on how to handle incidents that may affect the security of your installation and the POB. This procedure is not intended to cover work related deaths offshore but does provide information on sudden death i.e. death as a result of violence, suicide and unknown or suspicious causes². Specific advice is contained within the appendices of this procedure (details below). You should remember; however, your primary responsibility is to secure the safety of the installation and its personnel.

When you are alerted to an incident you should contact your onshore team as soon as possible and wait for their instruction. They will contact the Police for you. In the meantime you should:

1. Get the major incident box (which is found []);
2. Secure the safety of the installation and personnel (see below for powers of restraint). Wherever possible, all personnel should be removed from the scene;
3. Contain and preserve the scene – the scene should be protected from unauthorised entry and the elements. You should:
 - **Preserve** – if weather is affecting the scene then take the cover sheet from the major incident box and cover as large an area as possible over the scene taking into account the safe running of the installation. If the matter is not time critical/weather dependent, then the onshore team should be consulted;
 - **Isolate** – you should protect the area from unauthorised entry by cordoning off the area and locking doors (if possible). This should not, however, compromise the crew's safety;
 - **Secure** - ensure the area is secure; for example, using available staff (that are not involved in the incident) to watch on areas where others could enter the scene. If the scene is distressing, all efforts should be made to prevent crew members viewing the scene; and
 - **Evidence** – do not touch or move any evidence unless absolutely necessary. Make sure you keep a log of all evidence at the scene and, if you need to move some of the evidence, contact the onshore team; and
 - **People** – take a note of who was at the scene when you arrived and who has been involved in containing and preserving the scene.

Once you have completed these actions you should not do anything further until you receive instructions from the onshore team or the Police arrive.

Powers of restraint

The law gives you the power to restrain someone offshore to secure the safety of the rest of the personnel on the installation. You should only restrain a person as a last resort and use the minimum amount of force required (otherwise you may face criminal allegations).

If you restrain a person then you should notify the onshore team immediately and make sure that all of your actions are recorded in the incident log book including:

² On occasions, it may be difficult to determine whether an incident is a health and safety work related incident. In such circumstances then the scene should be contained and preserved. Further guidance should be sought from the onshore team

- the conduct of the restrained person;
- the methods you used prior to restraint;
- the method of restraint;
- details of those who assisted; and
- the outcome.

Handling personnel

Witnesses – try and make a list of personnel who may have witnessed the incident, either directly or indirectly. You may want to suggest to witnesses that they do not discuss what they saw with others and, for their own record, make a note of what they saw while it remains fresh in their minds.

Suspects – the identification of a suspect is a matter for the Police but where there is an obvious suspect you may wish to ask that person to agree to remain separate from others on the installation and agree to be accompanied by at least two people to ensure that evidence is not tampered with or destroyed.

No further action should be taken until you have received instructions from the onshore team or the Police arrive.

7 Cyber Security

The risk to information and computer assets comes from a broad spectrum of threats with a broad range of capabilities. The impact (and therefore the harm) on your business will depend on the opportunities you present to an attacker (in terms of the vulnerabilities within your systems), the capabilities of the attackers to exploit them, and ultimately their motivation for attacking you.

The motivation of an attacker can vary from demonstrating their technical prowess for personal kudos, financial gain, commercial advantage, political protest; through to economic or diplomatic advantage for their country.

Whilst attackers may have the capability and the motivation, they still need an opportunity to deliver a successful attack. You have no control over their capabilities and motivations, but you can make it harder for attackers by reducing your vulnerabilities.

As part of your risk management processes, you should be assessing whether you are likely to be the victim of a targeted or un-targeted attack; every organisation connected to the Internet should assume they will be a victim of the latter. Either way, you should implement basic security controls consistently across your organisation, and where you may be specifically targeted, ensure you have a more in-depth, holistic approach to cyber security.

7.1 The Main Threats

Based on the intelligence provided to Police Scotland the main cyber threats to business are:

BUSINESS EMAIL COMPROMISE (BEC) - In a BEC, the attacker accesses the organisation's email system, often via a phishing email, in order to impersonate the member of staff and defraud the company, its employees or its customers. This is done through a number of means, such as issuing bogus invoices or impersonating the CEO and requesting emergency payments.

SPEAR PHISHING: phishing is generally untargeted mass emails sent to many people asking for sensitive information or encourage them to visit a fake website. Spear phishing messages are designed to do the same thing, however they are more highly focused and personalised to their victim and will appear to come from a trusted source, even someone in the same company.

RANSOMWARE: a piece of malicious software, often delivered via a phishing email, which makes data or systems unusable until the victim makes a payment.

DISTRIBUTED DENIAL OF SERVICE ATTACK (DDoS): where multiple systems, often infected with a virus, work together to target a single system causing a denial of service attack.

The access point for these cyber-attacks can be via one person's computer which, due to being connected to your network, can compromise your entire system. These threats are not unique to your business back onshore and can easily compromise your systems offshore too.

Key to keeping your network safe is user education and awareness. Your staff have a critical role to play in your organisation's security and so it's important that security rules and the technology provided enable users to do their job as well as help keep the organisation secure. This can be supported by a

systematic delivery of awareness programmes and training that deliver security expertise as well as helping to establish a security-conscious culture.

For more information on the cyber-threats to business and how you can better protect yourself please visit the National Cyber Security Centre website – www.ncsc.gov.uk. Onshore training for staff is also available from Police Scotland's Cybercrime Prevention Unit who can be contacted on SCDCyberPreventionNorth@Scotland.pnn.police.uk.

8 Firearms Guidance

Under terms of Sections 1 and 2 of the Firearms Act 1968, it is an offence to purchase or acquire, or have in your possession a firearm, shotgun or ammunition as defined under section 1 of the aforementioned act without having in force a certificate authorising you to do so.

If you are able to access or have the means to access (i.e. key control function) any firearm, shotgun or relevant ammunition, you are also required by law to be in possession of such a certificate. The individual must have a good reason for each of the weapons and ammunition that is held on that certificate.

Weapons used within the Energy Industry, for the purpose of igniting flares, require either a firearm or shotgun certificate or both dependent on circumstances

8.1 Firearms

Section 57 of the Firearms Act 1968 defines a firearm as a lethal barrelled weapon of any description from which any shot, bullet or other missile can be discharged and includes—

- any prohibited weapon, whether it is such a lethal weapon as aforesaid or not; and
- any component part of such a lethal or prohibited weapon; and
- any accessory to any such weapon designed or adapted to diminish the noise or flash caused by firing the weapon;

Any person who **uses** company firearms for gas flare ignition purposes or who has unrestricted access to the secure storage of those firearms **must** have a firearm certificate or a shotgun certificate or both depending on circumstances.

A smooth barrelled gun (shotgun) with a barrel of less than 24" in length is classified as a firearm and requires a firearm certificate to possess, this includes flare pistols. Each firearm to which an employee has access must be listed on their personal firearm certificates in line with Police Scotland policy.

8.1.1 Flare Ignition ammunition

Flare ignition ammunition is classified as prohibited ammunition and can only be possessed, purchased or acquired with a valid firearm certificate.

8.1.2 Shotgun Certificates

Section 1(3) of the Firearms Act 1968 defines a shotgun within the meaning of this Act, that is to say a smooth-bore gun (not being an air gun) which—

- has a barrel not less than 24 inches in length and does not have any barrel with a bore exceeding 2 inches in diameter;
- either has no magazine or has a non-detachable magazine incapable of holding more than two cartridges; and
- is not a revolver gun

Any person who **uses** company shotguns for offshore flare ignition purposes or who has **unrestricted access** to the secure storage of those shotguns **must** have a shotgun certificate.

A smooth bore gun with a barrel of more than 24" in length and which exceeds 48" in overall length is classified as a shotgun and requires a shotgun certificate to possess. Each shotgun to which an employee has access must be listed on their personal shotgun certificate.

Failure to securely store a shotgun or firearm when not in use is a criminal offence.

In practical term – this means an OIM or other member of staff CANNOT have any access to a Firearm/Shogun/ammunition without having a valid certificate. This includes 'constructive' possession – for example an OIM having the firearm or ammunition cabinet keys on their possession.

8.2 Security

All guns and ammunition must be secured within a British Standard (BS) Gun Cabinet when not in use. The cabinet must be firmly affixed to the fabric of the building or platform where they are to be stored. The keys to the cabinet should be also be secured to prevent unauthorised access and the most effective way to do so is by installing an approved 'Keysafe' to which only approved certificate holders would have access.

Guns and ammunition cannot be stored together but must be secured in separate locking BS cabinets. When acquiring a new weapon, consideration should be given to where that weapon is to be secured prior to shipping to its destination platform or base. Failure to secure guns or ammunition when not in use is a criminal offence.

8.3 Cancellation of Certificates

When an employee leaves a company, their 'good reason' to possess a firearm or shotgun certificate authorising their use of company guns ends. When this occurs, the firearm and/or shotgun certificate should be sent to the firearms licensing department for cancellation without delay. A short letter explaining the reason for cancelling the certificate should be enclosed with the certificate(s). Their employing company (usually the master certificate holder) should also then advise the firearms licensing department by e-mail or in writing that an employee has left their company.

8.4 Standard Operating Procedures

If not already in place, best practise would be for each company to compile and document a standard operating order for their processes and procedures for the acquisition and safe use of flare ignition guns and ammunition.

8.5 Further Information

If you require further information, the Police Scotland website has wealth of information available to the public in reference to Firearms Licensing in Scotland. This information can be accessed by using the following link

www.scotland.police.uk/about-us/finance/service-fees-and-charges/firearms/s.

Furthermore, a Guidance for Oil and Gas Industry- *Flare Firearms Procedure document* can be found within the Publications section of the EPOL webpage.

www.epolgroup.co.uk

Contact

Should you wish to contact the firearms licencing department, to discuss any aspect of licencing, please do so via the following email address:

FirearmsLicensinginverness@scotland.pnn.police.uk

9 Appendix

The Following pages of these guidelines contain template procedures that, in the opinion of the authors of these guidelines, should be sufficient in handling a variety of security incidents. Operators are, however, encouraged to have regard to their content and adapt as necessary.

Appendices

A Bomb Threat Procedures

The likelihood of a credible bomb threat to an offshore asset is low; however it is important that processes and procedures are put in place for dealing with this unlikely event. In the first instance, onboard staff will always have the responsibility to carry out initial searches.

Prompt and decisive actions combined with concurrent activity are vital elements in dealing effectively with bomb threats. Although these procedures are displayed sequentially wherever possible they should be carried out concurrently. An example may be that the notification and search procedures can be conducted at the same time.

Notification of the Threat

- Notification of a bomb/attack could come from a number of possible sources:
- Police - Who have received information that an explosive device has been planted.
- Staff member - Who has found a suspicious item or who has received a suspicious postal item.
- Telephone message - An individual or switchboard operator receives a telephone bomb threat, either to the asset or other premises or via a third party.
- Electronic message - An individual receives a threat via e-mail, text message or messenger etc.

Alerting the Authorities

You may receive a message that your own asset is at risk. In such cases, you or the deputy OIM has to decide how to respond.

Terrorists and extremists may give telephone warnings of bomb threats. Far more common is the bomb hoax caller who attempts to disrupt business and frighten staff with a spurious bomb threat.

In all cases, whether you consider the threat credible or not, your primary consideration must always be the safety of your staff:

- Contact your company onshore Incident Response Team/Duty Manager. Provide as much information as possible so that they can contact the Police.

Obtaining Accurate Information

In the unlikely event that a bomb threat is received directly by the asset should there be an opportunity to ask questions, try to ascertain further details ensuring that you record them accurately. If something is misheard, ask the caller to repeat the information. Ask the following:

- Where is the bomb?
- What time will it go off?
- What does it look like?

- What kind of bomb is it?
- Why are you doing it?
- Who are you?

Try to note anything at all about the caller including sex, general manner (aggressive/calm) type of voice, accent, mannerisms or idiosyncrasies and background noise³.

Making the Decision to Evacuate

When faced with a threat offshore there are four options:

1. Do nothing

This should only be adopted if you are certain that the call is a hoax, but you should contact the onshore team first. If in doubt, one of the other options should be utilised. Regardless of your assessment, the incident should be referred to the Police who will investigate.

2. Search and Partial Evacuation

Depending on the size and location of any suspicious object which has been located, you may consider a partial evacuation and retain essential staff and search teams.

3. Search and Evacuation (if necessary)

This is appropriate if the threat is assessed as non-credible. Staff trained and exercised in relation to search procedures and having knowledge of their surroundings, should search the location, especially muster points and routes leading to these. Treat any suspect object with extreme caution. If nothing is found, you may decide to declare the location safe. The Police will provide further advice if the threat is of a timed explosion and nothing has been found during the search.

4. Immediate Evacuation

If a bomb threat is received which you, after consultation with company/Police, indicates the existence of a high risk; there will be a case for evacuation as quickly as possible.

N.B. Evacuation as defined by The Offshore Installation (Prevention of Fire and Explosion, and Emergency Response) Regulations 1995, means “the leaving of an installation and its vicinity in a systematic manner without directly entering the sea”. The Maritime and Coastguard Agency (MCA) has an important role to play in facilitating such an evacuation.

Search Procedures and Methods

- **Search Plans** - It is vital to have search co-ordination plans prepared in advance and staff trained in their implementation. The objective of the plans is to ensure that the facility is checked as quickly and effectively as possible. This should happen concurrently with the notification process.

³ Police Scotland periodically runs an Offshore Security Awareness Course OIMs. Energy Industry Liaison Unit Police Scotland can provide further details

- **Search Sectors** - Where practical, facilities should be divided into sectors or areas. Priority should be given to the searching of common and easily accessible areas, and those areas which may be used for muster.
- **Search Teams** – The search team should be formed from staff familiar with the area. The numbers required will depend on the size of the search task. These staff should be trained and rehearsed. It is vital they know that they are searching for an unidentified object that:
 - Should not be there;
 - Cannot be accounted for; or
 - Is out of place.
- **Report** - Immediately after the search has been completed or a suspicious object has been found, the results should be reported to you.

If a suspect device is found, you should be notified immediately and the following action taken:

- Do not move or touch the object;
- If possible leave a distinct marker near the object;
- Mark a route to the device if possible;
- Move personnel away from the object; and
- Advise Police and onshore response team immediately.

The Police will want to know the following information, known as the five W's:

- What is it? (the finder should memorise a description - size, shape, colour etc)
- Where is it? (exact location - access points)
- Why is it suspicious?
- When was it found?
- Who found it? (It is important that those with knowledge of the device can be contacted by the Police.)
- **Continuous Liaison** – you should keep in regular contact with the Police and Incident Response Team/Duty Manager.
- **All Clear?** - If nothing suspicious is found, in consultation with the Police and incident management, you will give the all clear.

B Suspect Package / Item

In the unlikely event that a suspicious item arrives on-board the following provides guidance on managing the incident:

What to look for in a postal item

The following table gives indicators, which might cause you to be suspicious of a letter or package. It is not exhaustive but will help you be aware of the possibilities:

If in any doubt, treat the item as potentially dangerous.

Identifier	What to look for
Address	Wrongly addressed or from an unexpected source.
Grease	Grease marks on the envelope or wrapping.
Shape	Visible wiring or tin foil, especially if the wrapping or envelope is damaged. Unusual shape for normal mail.
Size and Weight	Heavy for its size. Weight distribution uneven. Contents rigid in a flexible envelope.
Smell	An unusual odour such as marzipan or machine oil.
Source	Envelope or package delivered from an unknown source.
Spelling	Poor handwriting, spelling or typing. Stencils used for address.
Stamps	Too many stamps for weight.
Wrapping	Package has excessive wrapping.

What to do with a suspicious item If at any time, you are suspicious of an item:

- Identify sender - Try to get the recipient and sender to confirm if the package is legitimate.
- Don't handle any more than is necessary.
- Contact your company – Onshore Incident Response Team/Duty Manager. Provide as much information as possible so that they can contact the Police.
- Clear the area of staff, ideally out of line of sight (the distance will depend on the size of the possible device and local circumstances).
- Prevent the use of mobile phones and radios in the immediate proximity of the suspect item.
- Flat Surface - Place the device on a flat surface.

- Isolate/Cordon/Control - Ensure it is isolated and an appropriate cordon is established and controlled.
- NEVER cover the device or submerge in water.
- All clear - If the item is deemed harmless, in consultation with the Police and incident management, you will give the all clear. If this was deemed to be a deliberate hoax then evidential and crime scene management rules will apply.

C Drugs / Contraband Find

In the event of a suspect drugs or contraband find, the following general principles should always be followed until advice can be taken from the onshore team/Police:

Preserve

The incident scene should be protected from unauthorised entry using staff resources and barrier tape or similar. As large an area as possible should be protected taking into account the safe running of the installation.

Isolate

The area should be isolated provided this can be done without compromising the crew's safety and it is not critical to the ongoing operations of the installation.

Secure

Ensure the area is secure; for example, use your staff to maintain a watch at areas where others could enter the scene.

Evidence

Treat any incident scene with the utmost importance, and keep an incident log book. This will allow you to detail the course of action you have decided on.

Detailed Actions

Depending on the nature and scale of the incident and the circumstances of the find, the Police may attend the installation to carry out an investigation. Alternatively, the matter may be dealt with from onshore. In any case, you should consider the following actions:

- Contact your company - Onshore Incident Response Team/Duty Manager. Provide as much information as possible so that they can contact the Police.
- Log - Maintain an incident log book

Subject to advice:

- Photograph - The drugs/contraband.
- Bag – Contain the drugs and place them in a secure place.
- Audit Trail - Establish a written audit trail, especially if the drugs are transported onshore.

D Hostage Situation

In the event of a hostage situation, the primary consideration is always the safety of the hostage(s):

- External Influences - Ensure that there are no external influences that could impact upon the safety and security of the hostage or other staff.
- Contact the onshore team – they will contact the Police to obtain advice and guidance.
- Secure the area.
- Establish communications - With the hostage taker, without entering into negotiations.
- Log - Maintain a detailed log of issues in the incident log book.

E Sabotage / Criminal Damage

The Police may only become involved in the investigation of an act of sabotage, or criminal damage if it causes a significant amount of damage or poses a danger to life and limb. In this event the following actions should be taken:

Preserve

The incident scene should be protected from unauthorised entry using available staff resources, barrier tape or similar. As large an area as possible should be protected taking into account the safe running of the installation.

Isolate

The area should be isolated provided this can be done without compromising the crew's safety and it is not critical to the ongoing operations of the installation.

Secure

Ensure the area is secure; for example, use your staff to maintain a watch at areas where others could enter the scene. Where the scene is of a distressing nature, all efforts should be made to prevent crew members viewing the scene.

Evidence

Treat any incident scene with the utmost importance, and keep an incident log book. This will allow you to detail the course of action you have decided on. On their arrival, the Police will conduct a detailed examination of the crime scene and it is therefore essential that the above points are observed, as well as the following:

- Staff Safety - Carry out any actions which are required to ensure staff safety.
- Contact your company - Onshore Incident Response team/Duty Manager. Provide as much information as possible so that they can contact the Police.

Subject to advice:

- Photos - Take photos of the sabotaged equipment prior to repair.
- Log - Commence an incident log book detailing findings and actions
- Restrict Access - If possible prevent further access to scene and If possible prevent unrestricted access to other critical areas.

Note – If the damage requires immediate repair for safety reasons such repairs must be the priority. Any other damage should be left for examination by Police.

F Assault

In the event of an assault, depending on the severity and if appropriate, the following actions should be taken. It should be noted that the welfare of the victim is of primary concern.

Preserve

The incident scene should be protected from unauthorised entry using available staff resource, barrier tape or similar. As large an area as possible should be protected taking into account the safe running of the installation.

Isolate

The area should be isolated provided this can be done without compromising the crew's safety and it is not critical to the ongoing operations of the installation.

Secure

Ensure the area is secure; for example, use available staff to maintain a watch on areas where others could enter the scene. Where the scene is of a distressing nature, all reasonable efforts should be made to prevent crew members viewing the scene.

Evidence

Treat any incident scene with the utmost importance and keep an incident log book. This will allow you to detail the course of action you have decided on. On their arrival, the Police will conduct a detailed examination of the crime scene and it is therefore essential that the above points are observed, as well as the following:

- First Aid - Carry out any actions which are required to ensure the safety of staff, including administering first aid.
- Contact your company - Onshore Incident Response Team/Duty Manager. Provide as much information as possible so that they can contact the Police.

Subject to advice;

- Photos - Take photos of any injuries sustained.
- Weapons - If a weapon was involved, speak to the onshore team on how to ensure it is correctly preserved in the meantime.

G Illegal Occupation

This Appendix provides guidance in respect of protestor action, however you must be alert to the possibility of a terrorist attack. The Centre for Protection of National Infrastructure (CPNI) advises that initially any unauthorised intruder on the installation be considered a potential terrorist, unless intelligence indicates otherwise. In the event of an actual or imminent intrusion, operation of the platform should be immediately closed down to minimise potential risks.

Protestor Action

Environmental protests are normally peaceful and carried out by well trained and disciplined individuals. It must be fully understood that the company owes a 'duty of care' to the protestors. Individual companies will have their own detailed response plan. Your primary consideration is the safety and security of staff and the installation.

A strategic response to offshore protestor action can be found at: <http://www.oilandgasuk.co.uk/publications/viewpub.cfm?frmPubID=403>

This planning and response strategy is designed to cope with protesters arriving on the platform, by whatever means, and should be implemented in cognisance to the level of threat. All actions taken during the course of the incident will be consistent with the commitment of the company values such as:

- Health and Safety
- Environmental Considerations
- Ethics/Legislation
- Business Reputation

An offshore protest should be considered as:

- Essentially a safety issue that places the lives of staff and protestors at risk.
- Criminal – if protestors contravene Maritime Law or other legislation.
- Unlawful (in Civil Law) – if the protest action prevents the company carrying on its business.

Prevention

If there is a perceived risk of illegal intrusion, consideration should be given to:

- Access - Security of deck hatches and other deck access (lockdown).
- Key points - Security of key process control points e.g.:
 - Valves
 - Switch boxes
 - MAC points
- Robust access control measures.
- Response team - Placing the response team on standby.
- Briefing - To relevant crew members on the background of the protester organisation and of previous operations which they have mounted.

- Guidance - On staff behaviour during protester incidents with particular emphasis on safety, the requirement to negate sound-bite or photo opportunities and the necessity to adopt the highest standards of behaviour whilst dealing with protesters.
- Additional watches - The mounting of additional watches.
- Key Points - Additional security of vital areas, such as the bridge, control room, radio room and other key points.
- CCTV - Correct functioning of the CCTV system.

Response

- Be mindful of adverse media coverage generated by photo opportunities deliberately instigated by the protesters.
- Evidence gathering should be conducted in line with the response plan and in liaison with legal departments.
- Avoid being drawn or provoked into confrontational situations.
- Avoid becoming involved in situations that would put health, safety or lives at risk.
- Adopt a slow, deliberate and calm but firm approach.
- Display the highest standards of behavior when dealing with protesters.

Should intruders or protesters arrive on the platform suggested actions may include, but are not limited to:

- Immediate Emergency shutdown - This will minimise risk while the nature of the intrusion is determined.
- Contact your company - Onshore Incident Response Team/Duty Manager. Provide as much information as possible so that they can contact the Police.
- Safety - Provide full safety briefing in relation to the installation.
- Allocate a buddy - (e.g. an experienced safety rep from your crew) to remain with the protesters, ensure that the safety of any such person is not put at risk due to the movements of the protester(s).
- Personal details - Obtain full personal details of those involved and add to POB list.
- Reason - Try to ascertain the reason for the protest.
- Lock Down - Ensure that critical areas of the installation 'lock down' are maintained to prevent unauthorised access.
- Evidence - Video, photographic and audio evidence gathering (for internal purposes).
- Media - Refer any media enquires to the onshore response team.

Warning - The protesters should receive a warning that their actions may place themselves and others in danger. They must also be warned of the potential consequence of their actions. All warnings and reactions to them should be logged accordingly.

Power of Restraint

As mentioned previously in this document, you are granted the power of restraint when the health and/or safety of those on board, or the safety of the installation is put at risk. If you consider using this

power in relation to a protester, it is recommended that you seek advice from the Police, to ensure compliance with the regulations.

H Sudden Death

Definition

The term “sudden death” means any death as a result of violence, suicide and unknown or suspicious causes. In practice a sudden death is regarded as any death which is not preceded by illness or where illness is apparent but for only a short time prior to death. It is highly likely that any death that occurs offshore would fall under this description.

Any information included in this Appendix, does not supersede or take precedence over the ‘Offshore Installations (Logbook and Registration of Deaths) 1972.

<http://www.legislation.gov.uk/uksi/1972/1542/contents/made>

In the event of a sudden death, the following principles should always be considered before taking any actions:

Preserve

The incident scene should be protected from unauthorised entry using available staff resource, barrier tape or similar. As large an area as possible should be protected taking into account the safe running of the installation.

(Note that the Reporting of Incidents, Diseases and Dangerous Occurrences Regulation, RIDDOR 1995 Schedule 6 requires that where any person dies as a result of or in connection with work at an offshore workplace, no person shall disturb the place where it happened or tamper with anything at that place before the expiry of 3 clear days after the matter has been notified to HSE; or the place has been visited by an HSE inspector. Nothing shall prohibit the doing of anything by or with the consent of the HSE inspector, or the doing of anything necessary to secure the safety of the workplace or of any person, plant or vessel).

<https://www.hse.gov.uk/forms/incident/oir8.pdf> - Link to form to be completed in respect of the death or loss of a person pursuant to Regulation 9 of the Offshore Installations (Logbooks and Registration of Death) Regulations 1972 and sent direct to:

Register of Shipping PO Box 420

Cardiff CF24 5JW

Isolate

The area should be isolated provided this can be done without compromising the crew’s safety and it is not critical to the ongoing operations of the installation.

Secure

Ensure the area is secure; for example, use your available staff to maintain a watch on areas where others could enter the scene. Where the scene is of a distressing nature, all efforts should be made to prevent crew members viewing the scene. The cabin used by the deceased should also be secured as should all lockers he/she has access to.

Evidence

Treat any incident scene with the utmost importance, and keep an incident log book. This will allow you to detail the course of action you have decided on. On their arrival, the Police will conduct a detailed examination of the crime scene and it is therefore essential that the above points are observed.

Actions at the Scene

The saving of life is paramount to other considerations. Where a life is capable of being saved then this should be the primary consideration. It may be that the medic must take a course of action that may disturb the scene and, as such, the medic must be aware that any interference with the body or its surroundings may also alter the significance to be attached to other evidential items at the scene. If any such action is taken then it is imperative that the actions, and the reason for such actions, are recorded in the incident log book.

Notes - Upon notification, remain calm and take a note of how the body was discovered, by whom and exactly when.

Contact your company - Onshore Incident Response Team/Duty Manager. Provide as much information as possible so that they can contact the Police.

Subject to advice:

- Restrict Access - Take immediate measures to preserve the scene and surrounding area by ensuring access to the body and immediate area is restricted and that a careful record is taken of all persons who have come in to contact with it. This may require identifying an individual to act as a guard at the scene. Hanging - The saving of life will always be paramount. However, if a person has died and cannot be saved, do not disturb knots or any part of the scene.
- Identity - Take appropriate measures to confirm the identity of the subject and that life is extinct or otherwise. Time and person confirming needs to be recorded.
- Log - Ensure that an incident log book is commenced and diligently completed.
- Scene – Try and take note of the scene conditions in the incident log book, e.g., exact location, doors open/closed, locked/unlocked, heating on/off, electrical equipment on/off, any signs of disturbance, drawers open etc, visually and WITHOUT touching anything.
- People – Try and make a list of all known persons who have been at the scene with a brief description of what they were wearing.
- No Search - DO NOT conduct or allow any search of the scene and area, but preserve for law enforcement examination.
- Protective clothing - In the case of obvious serious injury and/or loss of bodily fluids, ensure that any person who may have been/is likely to come in to contact with it is provided with appropriate protective clothing or receives medical advice.
- Witnesses – Try and make a note of potential witnesses, e.g., cabin mates, last to have seen the subject etc.
- On board briefing - In consultation with onshore team, consider early internal communication strategy, i.e., what to tell personnel.

N.B If the death is witnessed and nothing suspicious has occurred, consideration could be given to moving the deceased to a more suitable area, whilst making sure the remainder of the original scene is preserved. Police advice must be obtained prior to taking this action.

I Armed Assailant Action

In the unlikely event that an armed assailant is on board your installation, if you can't evacuate, the next best option is to hide in a place where the armed intruder is not likely to find you. The place you choose to hide should be out of view; provide protection if shots are fired in your direction; should not trap you or restrict your options for movement. When hiding be sure to do the following:

- Lock all doors.
- Blockade the door with heavy furniture.
- Silence your radio and/or pager.
- Turn off any other source of noise such as a radio or television.
- Hide behind large items.
- Remain quiet and calm.
- Contact your onshore team – alert your onshore team, who will contact the Police. If you cannot speak just leave the line open for the operator to listen in.

Finally, and only as an absolute last resort, when evacuation and hiding options are not available and you are in danger, consideration may be given to take action against the armed intruder.

However, no person should place himself or another at risk by trying to tackle the assailant. The use of force may in itself lead to a worsening of a situation and can lead to a person's death or numerous deaths or injuries.

Force should not be used against an armed intruder unless there is a real and immediate danger of the loss of life or serious injury and no other option is available. Remember no more force than is necessary to achieve the overpowering and restraining of the assailant can be used.

Response

Be aware that the response team arriving on the scene may be heavily armed, possibly with rifles and shotguns, and may be wearing heavy outer bulletproof vests, helmets, and other tactical equipment. The response team may use pepper spray and/or tear gas. You should be aware of the following:

- Listen for and follow any instructions.
- Put down anything in your hands, including bags, jackets, mobile phones and keys.
- Immediately raise your hands and spread your fingers.
- Keep your hands visible at all times.
- Avoid making any quick movements.
- Avoid grabbing or attempting to hold onto the officers for their safety and yours.
- Do not make sudden movements towards the officers.
- Avoid screaming, pointing and yelling.
- Do not stop to ask officers for help or directions just proceed in the direction from where the officers came from.

Be aware that the initial response teams will not stop to aid injured victims.



oilandgasuk.co.uk/guidelines

OGUK Guidelines

Member companies dedicate specialist resources and technical expertise in developing these guidelines with Oil & Gas UK with a commitment to work together, continually reviewing and improving the performance of all offshore operations.

Guidelines are free for our members and can be purchased by non-members.

oilandgasuk.co.uk

info@oilandgasuk.co.uk

 [@oilandgasuk](https://twitter.com/oilandgasuk)

 [Oil & Gas UK](https://www.linkedin.com/company/oilandgasuk)

OGUK